Sturm bounds for Siegel modular forms of degree 2 and odd weights

Toshiyuki Kikuta and Sho Takemori

August 10, 2015

Abstract

We correct the proof of the theorem in the previous paper presented by the first named author, which concerns Sturm bounds for Siegel modular forms of degree 2 and of even weights modulo a prime number dividing $2 \cdot 3$. We give also Sturm bounds for them of odd weights for any prime numbers, and we prove their sharpness. The results cover the case where Fourier coefficients are algebraic numbers.

1   Introduction

Sturm [15] studied how many Fourier coefficients we need, when we want to prove that an elliptic modular form vanishes modulo a prime ideal. Its number is so called "Sturm bound". We shall explain it more precisely. For a modular form f, let Λ be the index set of the Fourier expansion of f. An explicitly given finite subset S of Λ is said to be a *Sturm bound* if vanishing modulo a prime ideal of Fourier coefficients of f at S implies vanishing modulo the prime ideal of all Fourier coefficients of f.

Poor-Yuen [11] studied initially Sturm bounds for Siegel modular forms of degree 2 for any prime number p. After their study, in [1], Choi, Choie and the first named author gave other type bounds with simple descriptions for them in the case of $p \geq 5$. Moreover, the first named author [7] attempted to supplement the case of $p \mid 2 \cdot 3$. However, there are some gaps in the proof (of Theorem 2.1 in subsection 3.1, [7]). It seems that its method can only give more larger bounds. Richter-Raum [13] gave some bounds for any p in the case of general degree and any weight. However, their bounds seem not to be sharp except the case of $p \geq 5$ and even weight in degree 2 case. An improvement of their bounds depends on the case of degree 2.

In this paper, we correct the proof of Theorem 2.1 in [7] by a new method. Namely we give the sharp Sturm bounds for Siegel modular forms of degree 2 and

even weight in the case of $p = 2, 3$. Moreover we give also the sharp bounds for them of odd weights modulo any prime number p. It should be remarked that, their sharpness become important to confirm congruences between two modular forms by numerical experiments, as the weights grow larger. Finally, we remark also that our results cover the case where Fourier coefficients are algebraic numbers.

2 Statement of the results

In order to state our results, we fix notation. For a positive integer n, we define the Siegel modular group Γ_n of degree n by

$$\Gamma_n = \left\{ \gamma \in \mathrm{GL}_{2n}(\mathbb{Z}) \mid {}^t\gamma J_n \gamma = J_n \right\},$$

where $J_n = \begin{pmatrix} 0_n & -1_n \\ 1_n & 0_n \end{pmatrix}$ and 0_n (resp. 1_n) is the zero matrix (resp. the identify matrix) of size n. For a positive integer N, we define the principal congruence subgroup $\Gamma^{(n)}(N)$ of level N by

$$\Gamma^{(n)}(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_n \mid \begin{matrix} a \equiv d \equiv 1_n \mod N \\ b \equiv c \equiv 0_n \mod N \end{matrix} \right\}.$$

Here a, b, c, d are $n \times n$ matrices. A subgroup $\Gamma \subset \Gamma_n$ is said to be a congruence subgroup if there exists a positive integer N such that $\Gamma^{(n)}(N) \subset \Gamma \subset \Gamma_n$. For a congruence subgroup Γ, we say Γ is of level N if $N = \min \left\{ m \in \mathbb{Z}_{\geq 1} \mid \Gamma^{(n)}(m) \subset \Gamma \right\}$. We define the Siegel upper half space $\mathbb{H}_n$ of degree n by

$$\mathbb{H}_n = \left\{ x + iy \mid x \in \mathrm{Sym}_n(\mathbb{R}), \ y \in \mathrm{Sym}_n(\mathbb{R}), \ y \text{ is positive definite} \right\},$$

where $\mathrm{Sym}_n(\mathbb{R})$ is a space of $n \times n$ symmetric matrices with entries in $\mathbb{R}$. For a congruence subgroup Γ and $k \in \mathbb{Z}_{\geq 0}$, a $\mathbb{C}$-valued holomorphic function f on $\mathbb{H}_n$ is said to be a (holomorphic) Siegel modular form of degree n, of weight k and of level Γ if $f((aZ + b)(cZ + d)^{-1}) = \det(cZ + d)^k f(Z)$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. If $n = 1$, we add the cusp condition. We denote by $M_k(\Gamma)$ the space of Siegel modular forms of weight k and of level Γ.

Any f in $M_k(\Gamma)$ has a Fourier expansion of the form

$$f(Z) = \sum_{0 \leq T \in \frac{1}{N}\Lambda_n} a_f(T) q^T, \quad q^T := e^{2\pi i \mathrm{tr}(TZ)}, \quad Z \in \mathbb{H}_2,$$

where T runs over all positive semi-definite elements of $\frac{1}{N}\Lambda_n$, N is the level of Γ and

$$\Lambda_n := \{ T = (t_{ij}) \in \mathrm{Sym}_n(\mathbb{Q}) \mid t_{ii}, \ 2t_{ij} \in \mathbb{Z} \}.$$

For simplicity, we write $T = (m, r, n)$ for $T = \begin{pmatrix} m & r/2 \\ r/2 & n \end{pmatrix} \in \frac{1}{N}\Lambda_2$ and also $a_f(m, r, n)$ for $a_f(T)$.

Let R be a subring of $\mathbb{C}$ and $M_k(\Gamma)_R \subset M_k(\Gamma)$ the R-module of all modular forms whose Fourier coefficients lie in R.

Let f_1, f_2 be two formal power series of the forms $f_i = \sum_{0 \leq T \in \frac{1}{N}\Lambda_n} a_{f_i}(T) q^T$ with $a_i \in R$. For an ideal I of R, we write

$$f_1 \equiv f_2 \mod I,$$

if and only if $a_{f_1}(T) \equiv a_{f_2}(T) \mod I$ for all $T \in \frac{1}{N}\Lambda_n$ with $T \geq 0$. If $I = (r)$ is a principal ideal, we simply denote $f_1 \equiv f_2 \mod r$.

Let K be an algebraic number field and $\mathcal{O} = \mathcal{O}_K$ the ring of integers in K. For a prime ideal $\mathfrak{p}$ in $\mathcal{O}$, we denote by $\mathcal{O}_{\mathfrak{p}}$ the localization of $\mathcal{O}$ at $\mathfrak{p}$. Under these notation, we have

Theorem 2.1. Let k be a non-negative integer, $\mathfrak{p}$ an any prime ideal and $f \in M_k(\Gamma_2)_{\mathcal{O}_{\mathfrak{p}}}$. We put

$$b_k = \begin{cases} \left[\frac{k}{10}\right] & \text{if } k \text{ is even,} \\ \left[\frac{k-5}{10}\right] & \text{if } k \text{ is odd.} \end{cases}$$

Here $[\cdot]$ is the Gauss symbol. For $\nu \in \mathbb{Z}_{\geq 1}$, assume that $a_f(m, r, n) \equiv 0 \mod \mathfrak{p}^\nu$ for all m, r, $n \in \mathbb{Z}$ with

$$0 \leq m, n \leq b_k,$$

and $4mn - r^2 \geq 0$, then we have $f \equiv 0 \mod \mathfrak{p}^\nu$.

Remark 2.2.   1. If k is even and $\mathfrak{p} \nmid 2 \cdot 3$, then the statement of the theorem was essentially proved by Choi, Choie and the first named author [1].

2. As mentioned in Introduction, in the case where $\mathfrak{p} \mid 2 \cdot 3$ and k is even, the first named author stated the same property in [7]. However, the proof has some gaps and its method can give only more larger bounds. We give a new proof in subsection 5.1.

3. We note that $M_k(\Gamma_2) = \{0\}$ if k is odd and $k < 35$.

4. Other type bounds also were given in [8].

By the result of [1] and a similar argument to them, we can prove the following.

Corollary 2.3. Let $\Gamma \subset \Gamma_2$ be a congruence subgroup with level N, $k \in \mathbb{Z}_{\geq 0}$ and $f \in M_k(\Gamma)_{\mathcal{O}_{\mathfrak{p}}}$. We put $i = [\Gamma_2 : \Gamma]$. For $\nu \in \mathbb{Z}_{\geq 1}$, assume that $a_f(m, r, n) \equiv 0 \mod \mathfrak{p}^\nu$ for all m, r, $n \in \frac{1}{N}\mathbb{Z}$ with
$$0 \leq m, n \leq b_{ki}.$$
and $4mn - r^2 \geq 0$, then we have $f \equiv 0 \mod \mathfrak{p}^\nu$.

In the case of level 1 (i.e., $N = 1$), our bounds are sharp. More precisely, the following theorem holds.

Theorem 2.4. Let $k \in \mathbb{Z}_{\geq 0}$ and p be a prime number. We assume $M_k(\Gamma_2) \neq 0$. Then there exists $f \in M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$ with $f \not\equiv 0 \mod p$ such that

$$a_f(m, r, n) = 0, \quad \text{for all } m, \ n \leq b_k - 1.$$

3 Notation

For a prime number p and a $\mathbb{Z}_{(p)}$-module M, we put

$$\widetilde{M} = M \otimes_{\mathbb{Z}_{(p)}} \mathbb{F}_p.$$

For an element $x \in M$, we denote by $\widetilde{x}$ the image of x in $\widetilde{M}$. For a $\mathbb{Z}_{(p)}$-linear map $\varphi : M \to N$, we denote by $\widetilde{\varphi}$ the induced map from $\widetilde{M}$ to $\widetilde{N}$ by φ. For $n \in \mathbb{Z}_{\geq 1}$, let Γ be a congruence subgroup of Γ_n. We denote $\widetilde{M_k(\Gamma)_{\mathbb{Z}_{(p)}}}$ by $\widetilde{M_k(\Gamma)}_{\mathbb{Z}_{(p)}}$. For a commutative ring R and an R-module M, we denote by $\mathrm{Sym}^2(M) \subset M \otimes_R M$ the R-module generated by elements $m \otimes m$ for $m \in M$. Let R be a $\mathbb{Z}_{(2)}$-algebra and M an R-module. We define an R-module $\wedge^2(M)$ by $\wedge^2(M) = \{x \in M \mid x^\iota = -x\}$. Here ι is defined by $\iota(m \otimes n) = n \otimes m$ for $m, \ n \in M$. Let q_1, q_{12}, q_2 be variables and $S = \{q_1^m q_{12}^r q_2^n \mid m, n \in \mathbb{Z}_{\geq 0}, r \in \mathbb{Z}\}$ be a set of Laurent monomials. We define an order of S so that $q_1^m q_{12}^r q_2^n \leq q_1^{m'} q_{12}^{r'} q_2^{n'}$ if and only if one of the following conditions holds.

1. $m < m'$.

2. $m = m'$ and $n < n'$.

3. $m = m'$ and $n = n'$ and $r \leq r'$.

Let K be a field and $f = \sum_{m,r,n} a_f(m, r, n) q_1^m q_{12}^r q_2^n \in K[q_{12}, q_{12}^{-1}][\![q_1, q_2]\!]$ a formal power series. If $f \neq 0$, let $q_1^{m_0} q_{12}^{r_0} q_2^{n_0}$ be the minimum monomial which appears in f, that is the minimum monomial of the set $\{q_1^m q_{12}^r q_2^n \mid a_f(m, r, n) \neq 0\}$. We define the leading term $\mathrm{ldt}(f)$ of f by $a_f(m_0, r_0, n_0) q_1^{m_0} q_{12}^{r_0} q_2^{n_0}$. We also define the leading term of an element of $K[\![q_1, q_2]\!] \setminus \{0\}$ by the inclusion $K[\![q_1, q_2]\!] \subset K[q_{12}, q_{12}^{-1}][\![q_1, q_2]\!]$. We regard $M_k(\Gamma_2)$ as a subspace of $\mathbb{C}[q_{12}, q_{12}^{-1}][\![q_1, q_2]\!]$ by $\sum_{T=(m,r,n) \in \Lambda_2} a_f(m, r, n) q^T \mapsto \sum_{m,r,n} a_f(m, r, n) q_1^m q_{12}^r q_2^n$. For $f \in M_k(\Gamma_2)$, we denote by $\mathrm{ldt}(f)$ the leading term of the Fourier expansion of f. For a field K, we regard $K[\![q]\!] \otimes_K K[\![q]\!]$ as a subspace of $K[\![q_1, q_2]\!]$ by $q \otimes 1 \mapsto q_1$ and $1 \otimes q \mapsto q_2$. For a subring R of $\mathbb{C}$ and a subset S of $\mathbb{C}[\![q_1, q_2]\!]$, we put

$$S_R = \left\{ f = \sum_{m,n} a_f(m, n) q_1^m q_2^n \in S \mid a_f(m, n) \in R \right\}.$$

4 Witt operators

For the proof of the main results, we use Witt operators. In this section, we define Witt operators and introduce basic properties of them.

4.1 Elliptic modular forms

Since images of Witt operators can be written by elliptic modular forms, we introduce some notation for elliptic modular forms.

For $k \in 2\mathbb{Z}$ with $k \geq 4$, we denote by $e_k \in M_k(\Gamma_1)$ the Eisenstein series of degree 1 and weight k. We normalize e_k so that the constant term is equal to 1. We define Eisenstein series e_2 of degree 1 and weight 2 by

$$e_2(q) = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n,$$

where $\sigma_1(n)$ is the sum of all positive divisors of n. As is well known, e_2 satisfies the following identify:

$$\tau^{-2} e_2(-\tau^{-1}) = \frac{12}{2\pi i \tau} + e_2(\tau).$$

We put $\Delta = 2^{-6} \cdot 3^{-3} (e_4^3 - e_6^2)$. Then Δ is the Ramanujan's delta function.

For $k \geq 2$, we define $N_k(\Gamma_1)$ as the space of $\mathbb{C}$-valued holomorphic functions f on $\mathbb{H}_1$ that satisfies the following three conditions:

1. $f(\tau + 1) = f(\tau)$.

2. There exists $g \in M_{k-2}(\Gamma_1)$ such that

$$\tau^{-k} f(-\tau^{-1}) = \frac{1}{2\pi i \tau} g(\tau) + f(\tau) \quad \text{for } \tau \in \mathbb{H}_1.$$

3. f is holomorphic at the cusp $i\infty$.

Since $f - e_2 g / 12 \in M_k(\Gamma_1)$ for above f, we have the following lemma.

Lemma 4.1.
$$N_k(\Gamma_1) = M_k(\Gamma_1) \oplus e_2 M_{k-2}(\Gamma_1).$$

For $M = M_k(\Gamma_1)$ or $N_k(\Gamma_1)$, we regard M as a subspace of $\mathbb{C}[\![q]\!]$ via the Fourier expansion.

For $k = 2, 4, 6, 12$, we define elements of $\text{Sym}^2(N_k(\Gamma_1))_{\mathbb{Z}}$ as follows:

$$x_k = e_k \otimes e_k, \text{ for } k = 2, 4, 6, \qquad x_{12} = \Delta \otimes \Delta, \qquad y_{12} = e_4^3 \otimes \Delta + \Delta \otimes e_4^3. \quad (4.1)$$

We define $\alpha_{36} \in \wedge^2(M_{36}(\Gamma_1))_{\mathbb{Z}}$ by

$$\alpha_{36} = x_{12}^2 (\Delta \otimes e_4^3 - e_4^3 \otimes \Delta).$$

4.2 Definition of Witt operators

For $k \in \mathbb{Z}_{\geq 0}$ and $f \in M_k(\Gamma_2)$, we consider the following Taylor expansion

$$f(Z) = W(f)(\tau_1, \tau_2) + 2W'(f)(\tau_1, \tau_2)\,(2\pi i \tau_{12}) + W''(f)(\tau_1, \tau_2)\,(2\pi i \tau_{12})^2 + O(\tau_{12}^3),$$

where $Z = \begin{pmatrix} \tau_1 & \tau_{12} \\ \tau_{12} & \tau_2 \end{pmatrix} \in \mathbb{H}_2$. We put $q_1 = \mathbf{e}(\tau_1), q_2 = \mathbf{e}(\tau_2)$ and $q_{12} = \mathbf{e}(\tau_{12})$. By definition, the following properties hold (see [16, §9]).

1. $W'(f) = 0$ if k is even and $W(f) = W''(f) = 0$ if k is odd.

2. $W(f) \in \mathrm{Sym}^2(M_k(\Gamma_1))$ if k is even and $W'(f) \in \wedge^2(M_{k+1}(\Gamma_1))$ if k is odd. Here we identify q_1 with $q \otimes 1$ and q_2 with $1 \otimes q$.

3. For $f \in M_k(\Gamma_2)$ and $g \in M_l(\Gamma_2)$, we have
$$W(fg) = W(f)W(g), \quad W'(fg) = W'(f)W(g) + W(f)W'(g).$$
Assume k and l are both even. Then we have
$$W''(fg) = W''(f)W(g) + W(f)W''(g). \tag{4.2}$$

4. For $f = \sum_{m,r,n} a_f(m, r, n) q_1^m q_{12}^r q_2^n \in M_k(\Gamma_2)$, we have
$$W(f) = \sum_{m,r,n} a_f(m, r, n) q_1^m q_2^n, \quad W'(f) = \frac{1}{2} \sum_{m,r,n} r a_f(m, r, n) q_1^m q_2^n,$$
$$W''(f) = \frac{1}{2} \sum_{m,r,n} r^2 a_f(m, r, n) q_1^m q_2^n.$$

Let k be even and $f \in M_k(\Gamma_2)$. Then we have

$$\tau_1^{-k-2} W''(f)(\tau_1^{-1}, \tau_2) = -\frac{1}{2\pi i} \theta_2 W(f)(\tau_1, \tau_2) + W''(f)(\tau_1, \tau_2),$$
$$W''(f)(\tau_1, \tau_2) = W''(f)(\tau_2, \tau_1).$$

Here $\theta_2 = \frac{1}{2\pi i} \frac{d}{d\tau_{12}}$. Therefore by Lemma 4.1, we have the following lemma.

Lemma 4.2. Let $k \in 2\mathbb{Z}_{\geq 0}$ and $f \in M_k(\Gamma_2)$. Then we have $W''(f) \in \mathrm{Sym}^2(N_{k+2}(\Gamma_1))$.

Let R be a subring of $\mathbb{C}$. If k is even and $f \in M_k(\Gamma_2)_R$, then we have

$$W''(f) = \sum_{\substack{m,r,n \\ r>0}} r^2 a_f(m, r, n) q_1^m q_{12}^r q_2^n,$$

since $a_f(m, -r, n) = a_f(m, r, n)$. Thus we have $W''(f) \in \mathrm{Sym}^2(M_k(\Gamma_1))_R$. By a similar reason, we have $W'(f) \in M_{k+1}(\Gamma_2)_R$ for $f \in M_k(\Gamma_2)_R$ with odd k. For $k \in \mathbb{Z}_{\geq 0}$, we define R-linear maps induced by W, W' and W'' as follows.

$$W_{R,2k} : M_{2k}(\Gamma_2)_R \to \mathrm{Sym}^2(M_{2k}(\Gamma_1))_R,$$
$$W'_{R,2k-1} : M_{2k-1}(\Gamma_2)_R \to \wedge^2(M_{2k}(\Gamma_1))_R,$$
$$W''_{R,2k} : M_{2k}(\Gamma_2)_R \to \mathrm{Sym}^2(N_{2k+2}(\Gamma_1))_R.$$

4.3 Igusa's generators and their images

Let X_4, X_6, X_{10}, X_{12} and X_{35} be generators of $\bigoplus_{k\in\mathbb{Z}} M_k(\Gamma_2)$ given by Igusa [4], [5]. Here X_4 and X_6 are Siegel-Eisenstein series of weight 4 and 6 respectively. And X_{10}, X_{12} and X_{35} are cusp forms of weight $10, 12$ and 35 respectively. We normalize these modular forms so that

$$\mathrm{ldt}(X_4) = \mathrm{ldt}(X_6) = 1, \quad \mathrm{ldt}(X_{10}) = \mathrm{ldt}(X_{12}) = q_1 q_{12}^{-1} q_2^2, \quad \mathrm{ldt}(X_{35}) = q_1^2 q_{12}^{-1} q_2^3.$$

Here we note that $a_{X_{35}}(1, r, n) = 0$ for all $n, r \in \mathbb{Z}$, because a weak Jacobi form of index 1 and weight 35 does not exist. We also introduce $Y_{12} \in M_{12}(\Gamma_2)_{\mathbb{Z}}$ and $X_k \in M_k(\Gamma_2)_{\mathbb{Z}}$ for $k = 16, 18, 24, 28, 30, 36, 40, 42$ and 48. Then by Igusa [6],

$$\big\{ X_k \mid k = 4, 6, 10, 12, 16, 18, 24, 28, 30, 36, 40, 42, 48 \big\} \cup \{Y_{12}\}$$

is a minimal set of generators of $\bigoplus_{k\in 2\mathbb{Z}} M_k(\Gamma_2)_{\mathbb{Z}}$ as a $\mathbb{Z}$-algebra and we have $M_k(\Gamma_2)_{\mathbb{Z}} = X_{35} M_{k-35}(\Gamma_2)_{\mathbb{Z}}$ for odd k.

Igusa [6] computed $W(X_4), \cdots, W(X_{48})$ and $W(Y_{12})$, we introduce some of them.

$$W(X_4) = x_4, \quad W(X_6) = x_6, \quad W(X_{10}) = 0,$$
$$W(X_{12}) = 2^2 \cdot 3 x_{12}, \quad W(Y_{12}) = y_{12}, \quad W(X_{16}) = x_4 \cdot x_{12} \tag{4.3}$$

and

$$W(X_{12i}) = d_i x_{12}^i, \text{ for } i = 1, 2, 3, 4. \tag{4.4}$$

Here x_4, x_6, x_{12} and y_{12} are defined by (4.1), and d_i is defined by $12/\gcd(12, i)$.

Images of W' and W'' for some of the generators are given as follows.

Lemma 4.3. We have
$$W'(X_{35}) = \alpha_{36}.$$

and
$$W''(X_{10}) = x_{12}, \quad W''(X_{12i}) = x_2 x_{12}^i, \text{ for } i = 1, 2, 3, 4.$$

Proof. By $\mathrm{ldt}(X_{35}) = q_1^2 q_{12}^{-1} q_2^3$ and $\wedge^2(M_k(\Gamma_1)) = (\Delta \otimes e_4^3 - e_4^3 \otimes \Delta)\mathrm{Sym}^2(M_{k-12}(\Gamma_1))$, we see that $W'(X_{35})$ is a constant multiple of α_{36}. Since $a_{X_{35}}(2, r, 3) = 0$ if $r \neq \pm 1$, we have $W'(X_{35}) = \alpha_{36}$. Igusa computed $W''(X_{10})$ and $W''(X_{12})$ (see [6, Lemma 12]). Note that our notation is different from his notation. We denote his W' by W''. By this result, we can compute $W''(X_{12i})$ for $i = 2, 3, 4$. $\square$

4.4 Kernel of Witt operator modulo a prime

Let p be a prime number and k even. We consider the kernel of the Witt operator modulo p:

$$\widetilde{W}_{\mathbb{Z}_{(p)}, k} : \widetilde{M_k}(\Gamma_2)_{\mathbb{Z}_{(p)}} \to \mathrm{Sym}^2(M_k(\Gamma_2))_{\mathbb{Z}_{(p)}} \otimes_{\mathbb{Z}_{(p)}} \mathbb{F}_p.$$

First we consider the case when $p \geq 5$. This case is easier.

Lemma 4.4. Let p be a prime number with $p \geq 5$. Then we have

$$\bigoplus_{k \in 2\mathbb{Z}_{\geq 0}} \mathrm{Sym}^2\left(M_k(\Gamma_1)\right)_{\mathbb{Z}_{(p)}} = \mathbb{Z}_{(p)}[x_4, \ x_6, \ x_{12}].$$

Proof. It is easy to see that $\mathrm{Sym}^2\left(M_k(\Gamma_1)_{\mathbb{Z}_{(p)}}\right) = \mathrm{Sym}^2\left(M_k(\Gamma_1)\right)_{\mathbb{Z}_{(p)}}$ (see the remark after Theorem 5.12 of [11]). Since $p \geq 5$, we have $\bigoplus_{k \in 2\mathbb{Z}_{\geq 0}} M_k(\Gamma_1)_{\mathbb{Z}_{(p)}} = \mathbb{Z}_{(p)}[e_4, \ e_6]$ (see [14]). We note that $\bigoplus_{k \in 2\mathbb{Z}_{\geq 0}} \mathrm{Sym}^2\left(M_k(\Gamma_1)_{\mathbb{Z}_{(p)}}\right)$ is generated by x_4, x_6 and $e_4^3 \otimes e_6^2 + e_6^2 \otimes e_4^3$ as an algebra over $\mathbb{Z}_{(p)}$. Then the assertion of the lemma follows from the equation

$$2^{12} \cdot 3^6 x_{12} = x_4^3 + x_6^2 - \left(e_4^3 \otimes e_6^2 + e_6^2 \otimes e_4^3\right).$$

$\square$

The following is a key lemma for the proof of Theorem 2.1 for $\mathfrak{p} \nmid 2 \cdot 3$. This lemma was also used in [1].

Lemma 4.5. Let $p \geq 5$ be a prime number and $k \in 2\mathbb{Z}_{\geq 0}$. Then we have

$$\ker\left(\widetilde{W}_{\mathbb{Z}_{(p)},k}\right) = \widetilde{X}_{10}\widetilde{M}_{k-10}(\Gamma_2)_{\mathbb{Z}_{(p)}}.$$

Proof. This lemma seems well-known. But for the sake of completeness, we give a proof. The inclusion $\widetilde{X}_{10}\widetilde{M}_{k-10}(\Gamma_2)_{\mathbb{Z}_{(p)}} \subset \ker\left(\widetilde{W}_{\mathbb{Z}_{(p)},k}\right)$ is obvious, because $W(X_{10}) = 0$. Take $f \in M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$ with $W_{\mathbb{Z}_{(p)},k}(f) \equiv 0 \bmod p$. By (4.3) and Lemma 4.4, $W_{\mathbb{Z}_{(p)},k}$ is surjective. Take $g \in M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$ so that $W_{\mathbb{Z}_{(p)},k}(f) = pW_{\mathbb{Z}_{(p)},k}(g)$. Then by [9, Corollary 4.2], there exists $h \in M_{k-10}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $f - pg = X_{10}h$. This completes the proof. $\square$

Remark 4.6. Since $W(X_{12}) = 12x_{12}$ and $M_2(\Gamma_2) = \{0\}$, the assertion of the lemma does not hold if $p = 2, 3$.

Next we consider the case where $p = 2, 3$. We recall the structure of the ring $\bigoplus_{k \in 2\mathbb{Z}} \widetilde{M}_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$.

Theorem 4.7 (Nagaoka [10], Theorem 2). Let $p = 2, 3$. For $f \in \widetilde{M}_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$, there exists a unique polynomial $Q \in \mathbb{F}_p[x, y, z]$ such that

$$\tilde{f} = Q(\widetilde{X}_{10}, \widetilde{Y}_{12}, \widetilde{X}_{16}).$$

The above Q for Igusa's generators are given as follows.

Lemma 4.8 (Nagaoka [10], proof of Lemma 1, Lemma 2). 1. Suppose $p = 2$, then we have

$$X_4 \equiv X_6 \equiv 1 \mod p, \qquad X_{12} \equiv X_{10} \mod p,$$
$$X_{18} \equiv X_{16} \mod p, \qquad X_{24} \equiv X_{10}X_{16} \mod p,$$
$$X_{28} \equiv X_{30} \equiv X_{16}^2 \mod p, \qquad X_{36} \equiv X_{10}X_{16}^2 \mod p,$$
$$X_{40} \equiv X_{42} \equiv X_{16}^3 \mod p, \qquad X_{48} \equiv X_{16}^4 + X_{10}X_{16}^3 + X_{10}^4 Y_{12} \mod p,$$
$$X_{35}^2 \equiv X_{10}^2 Y_{12}^2 X_{16}^2 + X_{10}^6 \mod p.$$

2. Suppose $p = 3$, then we have

$$X_4 \equiv X_6 \equiv 1 \mod p, \qquad X_{12} \equiv X_{10} \mod p,$$
$$X_{18} \equiv X_{16} \mod p, \qquad X_{24} \equiv X_{10}X_{16} \mod p,$$
$$X_{28} \equiv X_{30} \equiv X_{16}^2 \mod p, \qquad X_{36} \equiv X_{16}^3 + 2X_{10}^3 Y_{12} + X_{10}X_{16}^2 \mod p,$$
$$X_{40} \equiv X_{16}^3 + 2X_{10}^3 Y_{12} \mod p, \qquad X_{42} \equiv X_{16}^3 + X_{10}^3 Y_{12} \mod p,$$
$$X_{48} \equiv X_{10}X_{16}^3 + 2X_{10}^4 Y_{12} \mod p,$$

and

$$X_{35}^2 \equiv 2X_{10}X_{16}^4 + X_{10}Y_{12}^2 X_{16}^3$$
$$+ 2X_{10}^2 X_{16}^3 + X_{10}^2 Y_{12}^2 X_{16}^2 + 2X_{10}^3 Y_{12}X_{16}^2$$
$$+ 2X_{10}^4 Y_{12}^3 + X_{10}^4 X_{16}^2 + 2X_{10}^7 \mod p.$$

For later use, we prove the following lemma.

Lemma 4.9. Let $p = 2, 3$ and $k \in 2\mathbb{Z}_{\geq 0}$ with $12 \nmid k$. Then we have

$$\widetilde{M}_k(\Gamma_2)_{\mathbb{Z}_{(p)}} \subset \widetilde{M}_{k+2}(\Gamma_2)_{\mathbb{Z}_{(p)}}.$$

Proof. Take $f \in M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$. We show that there exists $g \in M_{k+2}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $f \equiv g \mod p$. We may assume f is an isobaric monomial of Igusa's generators of even weights, that is $X_4, \cdots, X_{48}$ and Y_{12}. If $f = X_k$ with $12 \nmid k$, then by Lemma 4.8, we have $\widetilde{f} \in \widetilde{M}_{k+2}(\Gamma_2)_{\mathbb{Z}_{(p)}}$. In fact, we have $X_{18} \equiv X_4 X_{16} \mod p$, $X_{42} \equiv X_{16}X_{28} \mod 2$, $X_{40} \equiv X_{42} + X_{10}^3 Y_{12} \mod 3$ and $X_{42} \equiv X_{16}X_{28} + X_{10}^2 X_{12}Y_{12} \mod 3$. If f is an isobaric monomial of weight k, then f contains some X_k with $12 \nmid k$. Therefore we have the assertion of the lemma. $\square$

Let $f \in M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$ with $p = 2, 3$. As we remarked before, $W(f) \equiv 0 \mod p$ does not imply the existence of $g \in M_{k-10}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $f \equiv X_{10}g \mod p$. Instead of Lemma 4.5, we have the following proposition.

Proposition 4.10. Let $p = 2, 3$ and $k \in 2\mathbb{Z}_{\geq 0}$.

1. Suppose $12 \nmid k$. Then we have

$$\ker\left(\widetilde{W}_{\mathbb{Z}_{(p)},k}\right) = \widetilde{X}_{10}\widetilde{M}_{k-10}(\Gamma_2)_{\mathbb{Z}_{(p)}}.$$

2. Suppose $k = 12n$ with $n \in \mathbb{Z}$ and $p = 2$. For $0 \le i \le n$ with $4 \nmid i$, we put $i = 4s + t$ with $t \in \{1, 2, 3\}$ and $m_i = X_{12t}X_{48}^s Y_{12}^{n-i}$. Then we have

$$\ker\left(\widetilde{W}_{\mathbb{Z}_{(p)},k}\right) = \bigoplus_{\substack{0 \le i \le n \\ 4 \nmid i}} \mathbb{F}_p \widetilde{m}_i \oplus \widetilde{X}_{10}\widetilde{M}_{k-10}(\Gamma_2)_{\mathbb{Z}_{(p)}}.$$

3. Suppose $k = 12n$ with $n \in \mathbb{Z}$ and $p = 3$. For $0 \le i \le n$ with $3 \nmid i$, we put $i = 3s + t$ with $t \in \{1, 2\}$. and $m_i = X_{12t}X_{36}^s Y_{12}^{n-i}$. Then we have

$$\ker\left(\widetilde{W}_{\mathbb{Z}_{(p)},k}\right) = \bigoplus_{\substack{0 \le i \le n \\ 3 \nmid i}} \mathbb{F}_p \widetilde{m}_i \oplus \widetilde{X}_{10}\widetilde{M}_{k-10}(\Gamma_2)_{\mathbb{Z}_{(p)}}.$$

Moreover, if $f \in M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$ with $12 \mid k$ and

$$W(f) \equiv W''(f) \equiv 0 \mod p,$$

then there exists $g \in M_{k-20}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $f \equiv X_{10}^2 g \mod p$.

Proof. Suppose $12 \nmid k$. Then by [6, Lemma 13], $W_{\mathbb{Z},k}$ is surjective. Therefore, $W_{\mathbb{Z}_{(p)},k}$ is surjective. We can prove $\ker\left(\widetilde{W}_{\mathbb{Z}_{(p)},k}\right) = \widetilde{X}_{10}\widetilde{M}_{k-10}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ by a similar argument to the proof of Lemma 4.5. Next assume $k = 12n$ with $n \in \mathbb{Z}$. For simplicity, we assume $p = 2$. We can prove the case when $p = 3$ in a similar way. Take $f \in M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$ with $W(f) \equiv 0 \mod p$. Put $d_i = 12/\gcd(12, i)$. By [6, Lemma 13], there exist $a_{i,j}, b_i, c_i \in \mathbb{Z}_{(p)}$ such that

$$W(f) = \sum_{0 \le i \le j < n} a_{i,j} x_4^{3(n-j)} x_{12}^i y_{12}^{j-i} + \sum_{\substack{0 \le i \le n \\ 4 \mid i}} b_i x_{12}^i y_{12}^{n-i} + \sum_{\substack{0 \le i \le n \\ 4 \nmid i}} c_i d_i x_{12}^i y_{12}^{n-i}.$$

By $x_4 \equiv 1 \mod p$ and $W(f) \equiv 0 \mod p$, we have $a_{i,j} \equiv b_i \equiv 0 \mod p$ for all i, j. Here we note that $\widetilde{x}_{12}$ and $\widetilde{y}_{12}$ are algebraically independent over $\mathbb{F}_p$. This is because $\mathrm{ldt}(x_{12}^i y_{12}^j) = q_1^i q_2^{i+j}$. By [6, Lemma 13], there exists $f' \in M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that

$$W(f') = \sum_{0 \le i \le j < n} \frac{a_{i,j}}{p} x_4^{3(n-j)} x_{12}^i y_{12}^{j-i} + \sum_{\substack{0 \le i \le n \\ 4 \mid i}} \frac{b_i}{p} x_{12}^i y_{12}^{n-i}.$$

By (4.4), there exists $u_i \in \mathbb{Z}_{(p)}^\times$ such that $W(m_i) = u_i d_i x_{12}^i y_{12}^{n-i}$. Therefore, there exist $a_i \in \mathbb{Z}_{(p)}$ such that $W(f - pf' - \sum_{\substack{0 \le i \le n \\ 4 \nmid i}} a_i m_i) = 0$. By [9, Corollary 4.2], there

10

exists $g \in M_{k-10}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $\widetilde{f} = \sum_i \widetilde{a}_i \widetilde{m}_i + \widetilde{X}_{10}\widetilde{g}$. Thus we have

$$\ker\left(\widetilde{W}_{\mathbb{Z}_{(p)},k}\right) = \sum_{\substack{0 \leq i \leq n \\ 4 \nmid i}} \mathbb{F}_p \widetilde{m}_i + \widetilde{X}_{10}\widetilde{M}_{k-10}(\Gamma_2)_{\mathbb{Z}_{(p)}}. \qquad (4.5)$$

We show that the sum (4.5) is a direct sum. Let $a_i \in \mathbb{Z}_{(p)}$ for $0 \leq i \leq n$ with $4 \nmid i$ and $g \in M_{k-10}(\Gamma_2)_{\mathbb{Z}_{(p)}}$. We put $f = \sum_i a_i m_i + X_{10}g$. By (4.2), we have

$$W''(m_i) \equiv W''(X_{12t})W(X_{48}^s Y_{12}^{n-i}) \equiv x_{12}^i y_{12}^{n-i} \mod p. \qquad (4.6)$$

Here we use $W(X_{12t}) \equiv 0 \mod p$ for $t = 1, 2, 3$ and $x_2 \equiv 1 \mod p$. By Igusa's computation, images of 14 generators $X_4, \cdots, X_{48}$ by W can be written as $\mathbb{Z}$-coefficient polynomials of x_4, x_6, x_{12} and y_{12}. By Lemma 4.3, we have $W''(X_{10}) = x_{12}$. Thus there exist $\alpha_{a,b,c,d} \in \mathbb{Z}_{(p)}$ such that

$$W''(X_{10}g) = x_{12}W(g) = \sum_{a,b,c,d} \alpha_{a,b,c,d} x_4^a x_6^b x_{12}^c y_{12}^d,$$

where summation index runs over $\left\{(a, b, c, d) \in \mathbb{Z}_{\geq 0}^4 \mid 4a + 6b + 12c + 12d = k + 2\right\}$. We assume $\widetilde{W}''_{\mathbb{Z}_{(p)},k}(\widetilde{f}) = \widetilde{W}''_{\mathbb{Z}_{(p)},k}(\sum_i \widetilde{a}_i \widetilde{m}_i + \widetilde{X}_{10}\widetilde{g}) = 0$. Then by (4.6) and $x_4 \equiv x_6 \equiv 1$ mod p, we have

$$\sum_i \widetilde{a}_i \widetilde{x}_{12}^i \widetilde{y}_{12}^{n-i} + \sum_{a,b,c,d} \widetilde{\alpha}_{a,b,c,d} \widetilde{x}_{12}^c \widetilde{y}_{12}^d = 0.$$

Since $4a + 6b = 0$ or $4a + 6b \geq 4$, the isobaric degree of $\widetilde{x}_{12}^c \widetilde{y}_{12}^d$ is not equal to k. Therefore we have $\widetilde{a}_i = 0$ for all i. This shows that the sum (4.5) is a direct sum. This also shows that if $f \in M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$ with $12 \mid k$ satisfies $W(f) \equiv W''(f) \equiv 0 \mod p$, then there exists $h \in M_{k-10}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $f \equiv X_{10}h \mod p$. By $W''(f) \equiv 0$ mod p, we have $W(h) \equiv 0 \mod p$. Since $12 \nmid k - 10$, there exists $h' \in M_{k-20}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $h \equiv X_{10}h' \mod p$. Therefore we have $f \equiv X_{10}^2 h' \mod p$. This completes the proof. $\qquad \square$

Corollary 4.11. Let $p = 2, 3$ and $f \in M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$ with $12 \mid k$. If $W(f) \equiv 0 \mod p$, then there exists $g \in M_{k-8}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $f \equiv X_{10}g \mod p$.

Proof. By Lemma 4.8, the statement for $f = m_i$ is true for all i. Then by Proposition 4.10, we have $f \equiv X_{10}(g + h) \mod p$ with $g \in M_{k-8}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ and $h \in M_{k-10}(\Gamma_2)_{\mathbb{Z}_{(p)}}$. By Lemma 4.9, we have our assertion. $\qquad \square$

5 Proof of the main results

In this section, we give proofs of Theorem 2.1, Corollary 2.3 and Theorem 2.4.

We have $\widetilde{M}_k(\Gamma_2)_{\mathcal{O}_{\mathfrak{p}}} = \widetilde{M}_k(\Gamma_2)_{\mathbb{Z}_{(p)}} \otimes_{\mathbb{F}_p} \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$. Therefore Theorem 2.1 is reduced to the case of $\mathcal{O}_{\mathfrak{p}} = \mathbb{Z}_{(p)}$, where p is a prime number. We also note that the statement

of Theorem 2.1 for $\nu \geq 2$ is reduced to the case of $\nu = 1$ by repeatedly using the result. This method was used in [12].

As we remarked before, the statement of Theorem 2.1 was proved in [1] if k is even and $p \geq 5$. Thus in this section, we assume $k \equiv 0 \mod 2$, $p = 2, 3$ or $k \equiv 1 \mod 2$.

First, we introduce the following notation, which is similar to mod p diagonal vanishing order defined by Richter and Raum [13]. Let $\widetilde{f}$ be a $\mathbb{F}_p$-coefficients formal power series as follows;

$$
\widetilde{f} = \sum_{\substack{m,r,n \in \mathbb{Q} \\ m,n,4mn-r^2 \geq 0}} \widetilde{a}_f(m,r,n) q_1^m q_{12}^r q_2^n \in \bigcup_{N \in \mathbb{Z}_{\geq 1}} \mathbb{F}_p[q_{12}^{1/N}, q_{12}^{-1/N}][\![q_1^{1/N}, q_2^{1/N}]\!].
$$

We define $v_p(\widetilde{f})$ by

$$
v_p(\widetilde{f}) = \sup \left\{ A \in \mathbb{R} \mid \begin{array}{l} \widetilde{a}_f(m,r,n) = 0, \\ \text{for all } m,r,n \in \mathbb{Q} \text{ with } 0 \leq m,n < A \end{array} \right\}.
$$

By definition, we have

$$
v_p(\widetilde{f}\widetilde{g}) \geq \max \left\{ v_p(\widetilde{f}), v_p(\widetilde{g}) \right\}, \tag{5.1}
$$

for $\widetilde{f}, \widetilde{g} \in \bigcup_{N \in \mathbb{Z}_{\geq 1}} \mathbb{F}_p[q_{12}^{1/N}, q_{12}^{-1/N}][\![q_1^{1/N}, q_2^{1/N}]\!]$. We note that $v_p(\widetilde{f}) > A$ is equivalent to $\widetilde{a}_f(m,r,n) = 0$ for all $m, n \leq A$, where $A \in \mathbb{R}$.

For the proof of Theorem 2.1, we introduce the following three lemmas.

Lemma 5.1. Let p be a prime number and $\widetilde{f} \in \widetilde{M_k}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ with $k \in \mathbb{Z}_{\geq 0}$. Then we have $v_p(\widetilde{X}_{10}\widetilde{f}) = v_p(\widetilde{f}) + 1$ and $v_p(\widetilde{X}_{35}\widetilde{f}) \geq v_p(\widetilde{f}) + 2$.

Proof. We regard $\widetilde{X}_{10}$ and $\widetilde{X}_{35}$ as images in the ring of formal power series $\mathbb{F}_p(q_{12})[\![q_1, q_2]\!]$. By the Borcherds product of X_{10} (cf. [3]), we have $\widetilde{X}_{10} = q_1 q_2 u$ where u is a unit in $\mathbb{F}_p(q_{12})[\![q_1, q_2]\!]$. Similarly, we have $\widetilde{X}_{35} = q_1^2 q_2^2 (q_1 - q_2) v$ for some unit v in $\mathbb{F}_p(q_{12})[\![q_1, q_2]\!]$ (cf. [2]). The assertion of the lemma follows from these facts. $\square$

Remark 5.2. It is not easy to give an upper bound for $v_p(\widetilde{X}_{35}\widetilde{f}) - v_p(\widetilde{f})$ because of the factor $q_1 - q_2$ in the Borcherds product of X_{35}.

Lemma 5.3. Let p be a prime number and

$$
f = \sum_{m,n \geq 0} a_f(m,n) q_1^m q_2^n \in (M_k(\Gamma_1) \otimes M_k(\Gamma_1))_{\mathbb{Z}_{(p)}}.
$$

If $a_f(m,n) \equiv 0 \mod p$ for all $m, n \leq [k/12]$, then $f \equiv 0 \mod p$. In particular, for $g \in M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$, we have $W(g) \equiv 0 \mod p$ if $v_p(\widetilde{g}) > [k/12]$ and $W'(g) \equiv 0 \mod p$ if $v_p(\widetilde{g}) > [(k+1)/12]$.

Proof. By the original Sturm's theorem [15], the map

$$\widetilde{M_k}(\Gamma_1)_{\mathbb{Z}_{(p)}} \hookrightarrow \mathbb{F}_p[\![q]\!]/(q^{[k/12]+1})$$

is injective. Therefore we have the following injective map

$$\mathrm{Sym}^2(M_k(\Gamma_1))_{\mathbb{Z}_{(p)}} \otimes_{\mathbb{Z}_{(p)}} \mathbb{F}_p = \mathrm{Sym}^2(\widetilde{M_k}(\Gamma_1)_{\mathbb{Z}_{(p)}})$$
$$\hookrightarrow F_p[\![q]\!]/(q^{[k/12]+1}) \otimes_{\mathbb{F}_p} F_p[\![q]\!]/(q^{[k/12]+1}).$$

Here we note that $\mathrm{Sym}^2(M_k(\Gamma_1)_{\mathbb{Z}_{(p)}}) = \mathrm{Sym}^2(M_k(\Gamma_1))_{\mathbb{Z}_{(p)}}$, as we remarked in the proof of Lemma 4.4. Since the image of $\widetilde{f}$ by this map vanishes, we have $\widetilde{f} = 0$. □

Lemma 5.4. We define $f_k \in M_k(\Gamma_2)_{\mathbb{Z}}$ for $k = 35, 39, 41, 43$ and 47 as follows.

$$f_{35} = X_{35}, \quad f_{39} = X_4 X_{35}, \quad f_{41} = X_6 X_{35}, \quad f_{43} = X_4^2 X_{35}, \quad f_{47} = X_{12} X_{35}.$$

Then $\mathrm{ldt}(f_k) = q_1^2 q_{12}^{-1} q_2^3$ for $k = 35, 39, 41, 43$ and $\mathrm{ldt}(f_{47}) = q_1^3 q_{12}^{-2} q_2^4$.

Proof. This follows from $\mathrm{ldt}(X_4) = \mathrm{ldt}(X_6) = 1$, $\mathrm{ldt}(X_{12}) = q_1 q_{12}^{-1} q_2$ and $\mathrm{ldt}(X_{35}) = q_1^2 q_{12}^{-1} q_2^3$. □

5.1 Proof of Theorem 2.1 for $p = 2, 3$ and even k

Let $p = 2, 3$, $k \in 2\mathbb{Z}_{\geq 0}$ and $f \in M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$. We assume

$$v_p(\widetilde{f}) > b_k, \tag{5.2}$$

where b_k is given in Theorem 2.1. We prove the statement of Theorem 2.1 by the induction on k. First, we assume $k < 10$. Then the statement is true because $M_k(\Gamma_2)$ for $k = 4, 6, 8$ is one-dimensional and $\mathrm{ldt}(X_4) = \mathrm{ldt}(X_6) = \mathrm{ldt}(X_4^2) = 1$.

Next, we assume $k \geq 10$ and the statement is true if the weight is strictly less than k. By (5.2) and Lemma 5.3, we have $W(f) \equiv 0 \mod p$. If $12 \nmid k$, then by Proposition 4.10, there exists $g \in M_{k-10}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $f \equiv X_{10}g \mod p$. By (5.2) and Lemma 5.1, we have $v_p(\widetilde{g}) > b_{k-10}$. By the induction hypothesis, we have $g \equiv 0 \mod p$. Thus we have the assertion of Theorem 2.1 in this case. Next we assume $12 \mid k$. Then by Corollary 4.11, there exists $g \in M_{k-8}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $f \equiv X_{10}g \mod p$. Since $b_{k-10} \geq [(k-8)/12]$ for $k \geq 10$, we have $W(g) \equiv 0 \mod p$ by (5.2), Lemma 5.1 and Lemma 5.3. Therefore $W''(f) \equiv x_{12}W(g) \equiv 0 \mod p$. By Proposition 4.10, there exists $h \in M_{k-20}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $f \equiv X_{10}^2 h \mod p$. Since $v_p(\widetilde{h}) > b_{k-20}$, we have $h \equiv 0 \mod p$ by the induction hypothesis. Thus we have $f \equiv 0 \mod p$. This completes the proof. □

5.2 Proof of Theorem 2.1 for the case $p \nmid 2 \cdot 3$ and odd k

Let p be a prime number with $p \geq 5$ and $f \in M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$ with k odd. We assume

$$v_p(\widetilde{f}) > b_k. \tag{5.3}$$

We prove the theorem by the induction on k. Note that $M_k(\Gamma_2) = \{0\}$ if k is odd and $k < 35$ or $k = 37$. First assume that $0 \leq k - 35 < 10$ with $k \neq 37$. Then $M_k(\Gamma_2)$ is one-dimensional and spanned by f_k given in Lemma 5.4. By Lemma 5.4, the assertion of the theorem holds if $k - 35 < 10$.

Next we assume $k - 35 \geq 10$ and the assertion of the theorem holds if the weight is strictly less than k. By Igusa [6], there exists $g \in M_{k-35}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $f = X_{35}g$. By Lemma 4.3, we have

$$W'(f) = W'(X_{35})W(g) = \alpha_{36}W(g). \tag{5.4}$$

By $[(k+1)/12] \leq b_k$ and Lemma 5.3, we have $W'(f) \equiv 0 \bmod p$. Therefore, we have $W(g) \equiv 0 \bmod p$ by (5.4). Then by Lemma 4.5, there exists $g' \in M_{k-45}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $g \equiv X_{10}g' \bmod p$. We put $f' = X_{35}g'$. Then we have $f \equiv X_{10}f' \bmod p$. By (5.3) and Lemma 5.1, we have $v_p(\widetilde{f'}) > b_{k-10}$. By the induction hypothesis, we have $f' \equiv 0 \bmod p$. Thus $f \equiv 0 \bmod p$. This completes the proof. $\square$

5.3 Proof of Theorem 2.1 for $p = 2, 3$ and odd k

In this subsection, we assume $p = 2, 3$ and k is odd. Since the case when $k = 48 + 35 = 83$ is special in our proof, we prove the following two lemmas.

Lemma 5.5. Let $\widetilde{f} \in \widetilde{M}_{48}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ with $\widetilde{f} \neq 0$ and $\mathrm{ldt}(\widetilde{f}) = \alpha q_1^a q_{12}^b q_2^c$ be the leading term of $\widetilde{f}$. Here $\alpha \in \mathbb{F}_p^\times$. Assume $\widetilde{W}_{\mathbb{Z}_{(p)},48}(\widetilde{f}) = 0$. Then we have $a \leq 4$ and $c \leq 4$.

Proof. By Proposition 4.10, we have

$$\ker(\widetilde{W}_{\mathbb{Z}_{(p)},48}) = \bigoplus_i \mathbb{F}_p \widetilde{m}_i \oplus \widetilde{X}_{10}\widetilde{M}_{38}(\Gamma_2)_{\mathbb{Z}_{(p)}}.$$

Here $i = 1, 2, 3$ if $p = 2$ and $i = 1, 2, 4$ if $p = 3$. For $\widetilde{g} \in \widetilde{M}_{48}(\Gamma_2)_{\mathbb{Z}_{(p)}}$, let $Q_g = \sum_{a,b,c} \gamma_{a,b,c} x^a y^b z^c$ be a $\mathbb{F}_p$-coefficients polynomial such that $\widetilde{g} = Q_g(\widetilde{X}_{10}, \widetilde{Y}_{12}, \widetilde{X}_{16})$ as in Theorem 4.7. Since

$$\mathrm{ldt}\left(\widetilde{X}_{10}^a \widetilde{Y}_{12}^b \widetilde{X}_{16}^c\right) = q_1^{a+c} q_{12}^{-a} q_2^{a+b+c}, \tag{5.5}$$

there exists a unique monomial $\widetilde{X}_{10}^{a_0} \widetilde{Y}_{12}^{b_0} \widetilde{X}_{16}^{c_0}$ with $\gamma_{a_0,b_0,c_0} \neq 0$ such that $\mathrm{ldt}(\widetilde{g}) = \mathrm{ldt}(\gamma_{a_0,b_0,c_0} \widetilde{X}_{10}^{a_0} \widetilde{Y}_{12}^{b_0} \widetilde{X}_{16}^{c_0})$. We put $\phi(\widetilde{g}) = \widetilde{X}_{10}^{a_0} \widetilde{Y}_{12}^{b_0} \widetilde{X}_{16}^{c_0}$. We define a set S' by

$$\left\{ 1, \widetilde{X}_{16}, \widetilde{Y}_{12}, \widetilde{X}_{10}, \widetilde{X}_{16}^2, \widetilde{Y}_{12}\widetilde{X}_{16}, \widetilde{Y}_{12}^2, \widetilde{X}_{10}\widetilde{X}_{16}, \widetilde{X}_{10}\widetilde{Y}_{12}, \widetilde{X}_{10}^2, \right.$$
$$\left. \widetilde{X}_{10}\widetilde{X}_{16}^2, \widetilde{X}_{10}\widetilde{Y}_{12}\widetilde{X}_{16}, \widetilde{X}_{10}\widetilde{Y}_{12}^2, \widetilde{X}_{10}^2\widetilde{X}_{16}, \widetilde{X}_{10}^2\widetilde{Y}_{12}, \widetilde{X}_{10}^3 \right\}.$$

Then S' forms a basis of $\widetilde{M}_{38}(\Gamma_2)_{\mathbb{Z}_{(p)}}$. This follows from $\dim_{\mathbb{F}_p}(\widetilde{M}_{38}(\Gamma_2)_{\mathbb{Z}_{(p)}}) = \dim_{\mathbb{C}} M_{38}(\Gamma_2) = 16$ and Lemma 4.8. We put $S = \left\{ \widetilde{X}_{10}a \mid a \in S' \right\}$. We define a set T by

$$T = \begin{cases} \{\widetilde{m}_1, \widetilde{m}_2, \widetilde{m}_3\} & \text{if } p = 2, \\ \{\widetilde{m}_1, \widetilde{m}_2, \widetilde{m}_4\} & \text{if } p = 3. \end{cases}$$

Then $S \cup T$ forms a basis of $\ker(\widetilde{W}_{\mathbb{Z}_{(p)}, 48})$. We have $\phi(s) = s$ except when $p = 3$ and $s = m_4$ for $s \in S \cup T$. If $p = 3$, we have $\phi(\widetilde{m}_4) = \widetilde{X}_{10}\widetilde{Y}_{12}\widetilde{X}_{16}^2$. Thus we see that ϕ on $S \cup T$ is injective. Therefore if $\widetilde{f} \in \ker(\widetilde{W}_{\mathbb{Z}_{(p)}, 48})$ with $\widetilde{f} \neq 0$, then there exists a unique $s \in S \cup T$ such that $\mathrm{ldt}(\widetilde{f}) = \alpha \, \mathrm{ldt}(s)$ with $\alpha \neq 0$. Note that degrees of monomials $\{\phi(s) \mid s \in S \cup T\}$ are less than or equal to 4. Then by (5.5), we have the assertion of the lemma. $\qquad\square$

Lemma 5.6. Let $k = 83$, $\widetilde{f} = \widetilde{X}_{35}\widetilde{g} \in \widetilde{M}_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$ with $g \in \widetilde{M}_{k-35}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ and $\widetilde{W}_{\mathbb{Z}_{(p)}, k-35}(\widetilde{g}) = 0$. Assume $v_p(\widetilde{f}) > b_k = 7$. Then we have $\widetilde{f} = 0$.

Proof. Assume $\widetilde{f} \neq 0$. We put $\mathrm{ldt}(\widetilde{g}) = \alpha q_1^a q_{12}^b q_2^c$, where $\alpha \in \mathbb{F}_p^{\times}$. Then by Lemma 5.5, we have $a, c \leq 4$. Since $\mathrm{ldt}(\widetilde{X}_{35}) = q_1^2 q_{12}^{-1} q_2^3$, we have $\mathrm{ldt}(\widetilde{f}) = \alpha q_1^{a+2} q_{12}^{b-1} q_2^{c+3}$. By $a + 2 \leq 6$ and $c + 3 \leq 7$, we have $v_p(\widetilde{f}) \leq 7$. $\qquad\square$

Let k be odd and $f \in M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$. Assume that

$$v_p(\widetilde{f}) > b_k. \tag{5.6}$$

If $k < 45$, then the assertion follows from Lemma 5.4. Hence we suppose that $k \geq 45$. To apply an induction on k, suppose that the assertion is true for any weight strictly smaller than k.

We take $g \in M_{k-35}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $f = gX_{35}$. By (5.6), (5.4) and Lemma 5.3, we have $W(g) \equiv 0 \mod p$. Now we separate into four cases:

(1) If $k \not\equiv 11 \mod 12$, then there exists $g' \in M_{k-45}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $g \equiv X_{10}g' \mod p$, by Proposition 4.10. Then $f = X_{35}g = X_{35}X_{10}g'$. If we put $f' := X_{10}g' \in M_{k-10}(\Gamma_2)_{\mathbb{Z}_{(p)}}$, then

$$b_k < v_p(\widetilde{f}) = v_p(\widetilde{X}_{10}\widetilde{f'}) = 1 + v_p(\widetilde{f'}).$$

This implies $v_p(\widetilde{f'}) > b_{k-10}$. By the induction hypothesis, we get $f' \equiv 0 \mod p$. Therefore we have $f \equiv 0 \mod p$.

(2) If $k \equiv 11 \mod 12$ and $k \equiv 1, 5, 7, 9 \mod 10$, then we have $b_k = b_{k-8} + 1$. By Corollary 4.11, there exists $g' \in M_{k-43}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $g \equiv X_{10}g' \mod p$. Put $f' = X_{35}g' \in M_{k-8}(\Gamma_2)_{\mathbb{Z}_{(p)}}$. Then we have $v_p(\widetilde{f'}) = v_p(\widetilde{f}) - 1 > b_{k-8}$. By the induction hypothesis, we have $f' \equiv 0 \mod p$. Therefore we have $f \equiv 0 \mod p$.

(3) If $k \equiv 11 \mod 12$, $k \equiv 3 \mod 10$ and $k < 115$, then we have $k = 83$ because $k \geq 45$. Then by Lemma 5.6, we have $f \equiv 0 \mod p$.

(4) Finally, we assume $k \equiv 11 \mod 12$ and $k \geq 115$. To prove this case, we start with proving the following lemma.

Lemma 5.7. Let $f = X_{35}g \in M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$ with $W(g) \equiv 0 \mod p$. Assume $k \equiv 11 \mod 12$, $k \geq 115$ and (5.6). Then we have $W''(g) \equiv 0 \mod p$.

Proof. We show the statement only for $p = 2$. The case $p = 3$ also can be proved by a similar argument. By Corollary 4.11, there exists $g' \in M_{k-43}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $g \equiv X_{10}g' \mod p$. Then, it follows from Lemma 4.8 that

$$fX_{35} \equiv X_{10}X_{35}^2 g' \equiv g'X_{10}^3(Y_{12}^2 X_{16}^2 + X_{10}^4) \mod p.$$

By Lemma 5.1 and the assumption (5.6), we have

$$b_k + 2 < v_p(\widetilde{f}) + 2 \leq v_p(\widetilde{f}\widetilde{X}_{35}) = v_p(\widetilde{g}'\widetilde{X}_{10}\widetilde{X}_{35}^2) = 3 + v_p(\widetilde{g}'(\widetilde{Y}_{12}^2\widetilde{X}_{16}^2 + \widetilde{X}_{10}^4)).$$

This implies that

$$v_p(\widetilde{g}'(\widetilde{Y}_{12}^2\widetilde{X}_{16}^2 + \widetilde{X}_{10}^4)) > [(k-15)/10].$$

On the other hand, we have

$$W(g'(Y_{12}^2 X_{16}^2 + X_{10}^4)) = W(g'Y_{12}^2 X_{16}^2) \equiv W(g') \cdot y_{12}^2 \cdot x_{12}^2 \mod p,$$

where we used (4.3) and the fact $x_4 \equiv 1 \mod p$. By this congruence, $W(\widetilde{g}'(\widetilde{Y}_{12}^2\widetilde{X}_{16}^2 + \widetilde{X}_{10}^4))$ can be regarded as of weight $k - 43 + 48 = k + 5$. By $k \geq 115$, we have

$$v_p(\widetilde{g}'(\widetilde{Y}_{12}^2\widetilde{X}_{16}^2 + \widetilde{X}_{10}^4)) > [(k-15)/10] \geq [(k+5)/12].$$

Applying Lemma 5.3, we have

$$W(g'(Y_{12}^2 X_{16}^2 + X_{10}^4)) \equiv W(g') \cdot y_{12}^2 \cdot x_{12}^2 \equiv 0 \mod p.$$

This implies that

$$W''(g) \equiv W(g') \cdot x_{12} \equiv 0 \mod p.$$

This completes the proof of the lemma. $\qquad\square$

We shall return to proof of the case (4). Since $W(g) \equiv 0 \mod p$ and $W''(g) \equiv 0 \mod p$, there exists $h \in M_{k-55}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ such that $g \equiv X_{10}^2 h \mod p$ by Proposition 4.10. Note that $f \equiv X_{10}^2 X_{35}h \mod p$. If we put $f' := X_{35}h \in M_{k-20}(\Gamma_2)_{\mathbb{Z}_{(p)}}$, then

$$v_p(\widetilde{f}) = v_p(\widetilde{X}_{10}^2\widetilde{f}') = 2 + v_p(\widetilde{f}') > b_k.$$

This means that

$$v_p(\widetilde{f}') > b_{k-20}.$$

By the induction hypothesis, we get $f' \equiv 0 \mod p$. Therefore we have $f \equiv 0 \mod p$. This completes the proof. $\qquad\square$

16

5.4 Proof of Corollary 2.3

As explained in the beginning of this section, we may assume $\mathcal{O}_{\mathfrak{p}} = \mathbb{Z}_{(p)}$, where p is a prime number. Let $\Gamma \subset \Gamma_2$ be a congruence subgroup of level N and $f \in M_k(\Gamma)_{\mathbb{Z}_{(p)}}$. By the proof of [1, Theorem 1.3], there exists $g \in M_{k(i-1)}(\Gamma)_{\mathbb{Z}_{(p)}}$ such that

$$fg \in M_{ki}(\Gamma_2)_{\mathbb{Z}_{(p)}}, \text{ and } g \not\equiv 0 \mod p.$$

Here $i = [\Gamma_2 : \Gamma]$. We assume $v_p(\widetilde{f}) > b_{ki}$. Then by (5.1), we have

$$v_p(\widetilde{fg}) \geq v_p(\widetilde{f}) > b_{ki}.$$

By Theorem 2.1, we have $\widetilde{fg} = 0$. Since $\widetilde{g} \neq 0$, we have $\widetilde{f} = 0$, i.e., $f \equiv 0 \mod p$. This completes the proof. □

5.5 Proof of the sharpness

We prove Theorem 2.4. If k is even, then we can show the assertion of the theorem by a similar argument to [1]. Let k be odd and f_k for $k = 35, 39, 41, 43$ and 47 be modular forms given in Lemma 5.4. Then by Lemma 5.4, we have $\mathrm{ldt}(f_k X_{10}^i) = q_1^{2+i} q_2^{-1-i} q_3^{3+i}$ for $k = 35, 39, 41, 43$ and $\mathrm{ldt}(f_{47} X_{10}^i) = q_1^{3+i} q_2^{-2-i} q_3^{4+i}$. Thus we have the assertion of the theorem. □

Acknowledgment

References

[1] D. Choi, Y. Choie, and T. Kikuta, *Sturm type theorem for Siegel modular forms of genus 2 modulo p*, ACTA ARITHMETICA **158** (2013), no. 2, 129–139.

[2] V. A. Gritsenko and V. V. Nikulin, *Igusa modular forms and 'the simplest' Lorentzian Kac-Moody algebras*, Sbornik: Mathematics **187** (1996), no. 11, 1601.

[3] ———, *Siegel automorphic form corrections of some Lorentzian Kac-Moody Lie algebras*, American Journal of Mathematics (1997), 181–224.

[4] J. Igusa, *On Siegel modular forms of genus two*, American Journal of Mathematics (1962), 175–200.

[5] _____, *On Siegel modular forms of genus two (II)*, American Journal of Mathematics (1964), 392–412.

[6] _____, *On the ring of modular forms of degree two over* $\mathbb{Z}$, American Journal of Mathematics (1979), 149–183.

[7] T. Kikuta, *Remark on Sturm bounds for Siegel modular forms of degree 2*, Proceedings of the Japan Academy, Series A, Mathematical Sciences **91** (2015), no. 6, 82–84.

[8] T. Kikuta, H. Kodama, and S. Nagaoka, *Note on Igusa's cusp form of weight 35*, Rocky Mountain Journal of Mathematics **45** (2015), no. 3, to appear.

[9] S. Nagaoka, *Note on mod p Siegel modular forms*, Mathematische Zeitschrift **235** (2000), no. 2, 405–420.

[10] _____, *Note on mod p Siegel modular forms II*, Mathematische Zeitschrift **251** (2005), no. 4, 821–826.

[11] C. Poor and D. Yuen, *Paramodular cusp forms*, Mathematics of Computation **84** (2015), no. 293, 1401–1438.

[12] J. Rasmussen, *Higher congruences between modular forms*, Ph.D. thesis, University of Copenhagen, 2009.

[13] Olav K Richter and Martin Westerholt-Raum, *Sturm bounds for Siegel modular forms*, Research in Number Theory **1** (2015), no. 5.

[14] J. P. Serre, *Formes modulaires et fonctions zêta p-adiques*, Modular functions of one variable III, Springer, 1973, pp. 191–268.

[15] J. Sturm, *On the congruence of modular forms*, Number theory, Springer, 1987, pp. 275–280.

[16] G. Van Der Geer, *Siegel modular forms and their applications*, The 1-2-3 of modular forms, Springer, 2008, pp. 181–245.

Toshiyuki Kikuta
Faculty of Information Engineering
Department of Information and Systems Engineering
Fukuoka Institute of Technology
3-30-1 Wajiro-higashi, Higashi-ku, Fukuoka 811-0295, Japan
E-mail: kikuta@fit.ac.jp

Sho Takemori
Department of Mathematics, Hokkaido University
Kita 10, Nishi 8, Kita-Ku, Sapporo, 060-0810, Japan
E-mail: takemori@math.sci.hokudai.ac.jp